Manual de Usuario *Firewall*

INDICE

1. Introducción

Telefónica de España pone a su disposición ***Firewall,*** un producto que instalado en los equipos de su empresa le permite una protección avanzada para su ordenador y sus datos personales. Establece una barrera entre su equipo e Internet y controla el tráfico en busca de incidentes sospechosos.

Cuando Usted contrata licencias de ***Firewall*** en sus distintas modalidades de comercialización:

- ✓ *Firewall*
- ✓ *Pack Antivirus + Firewall*
- ✓ *Pack Seguridad Total (Antivirus + Firewall + Canguro Net Plus + Filtro de Correo)*

está adquiriendo licencias de uso y disfrute que protegen sus equipos.

2. Características.

El servicio presenta las siguientes características:

- Protege frente a posibles exploraciones y ataques de *hackers*
- Complementa las defensas antivirus
- Supervisa Internet y los inc identes de la red
- Alerta de incidentes potencialmente hostiles
- Ofrece información pormenorizada sobre el tráfico sospechoso por Internet
- Ofrece funciones de seguimiento detallado y búsqueda de incidentes.

inicio

3. Instalación y Configuración Inicial.

❑ **Sistemas Operativos.**

El servicio se ha diseñado para sistemas operativos *Microsoft Windows* que se ejecutan en plataformas PC. Se instala y funciona en servidores y estaciones de trabajo con:

- **Procesador:** Intel® Pentium® u otro de arquitectura compatible.
- **Navegador:** Microsoft Internet Explorer 6.0 o posterior
- **Estaciones de trabajo:** Windows 2000 Professional con Service Pack 3 o posterior, Windows XP Home o Professional (32 bits), Windows Vista (32 bits).
- **Servidores:** Windows 2000 Server con Service Pack 3 o superior, Windows 2000 Advanced Server con Service Pack 3 o superior, Windows 2000 Small Business Server con Service Pack 3 o superior, Windows 2003 Standard Server, Windows 2003 Enterprise Server, Windows 2003 Web Edition, Windows 2003 Small Business Server.
- **Requerimientos de RAM:** 256 MB mínimo recomendado (mínimo recomendado 512 MB para servidores y 1 GB para Windows Vista.)

❑ Instalación

Antes de instalar la funcionalidad ***Firewall***, guarde todo su trabajo y cierre las aplicaciones que tenga abiertas antes de continuar con los siguientes pasos para la instalación. El proceso es similar al de ***Antivirus***. Deberá reiniciar el ordenador como parte del proceso de instalación.

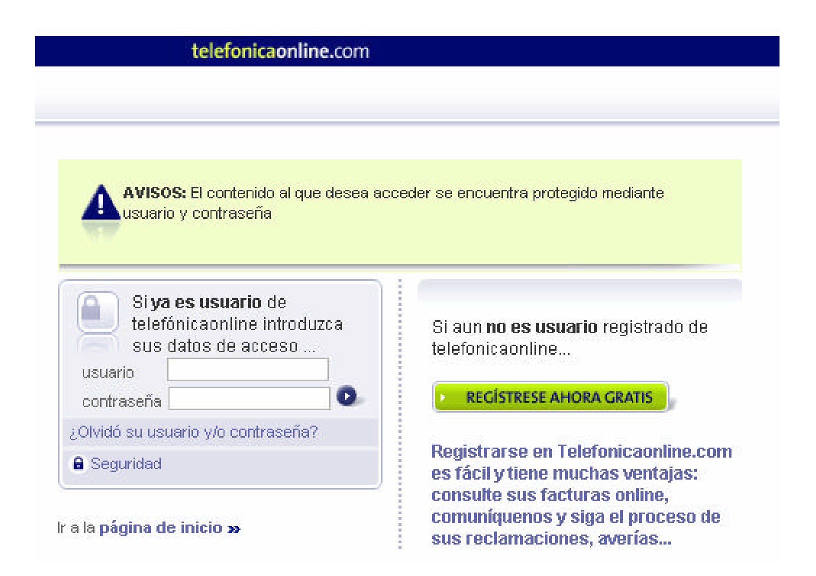
Si usted tiene contratado ***Firewall*** o ***Pack Antivirus + Firewall***, para instalar diríjase a la siguiente dirección web:

https://centroseguridad.solucionesadsl.telefonica.terra.es

e introduzca el usuario y contraseña proporcionado para el servicio.

Si usted es usuario de Pack Seguridad Total, para instalar:

1. Diríjase a www.telefonicaonline.com/packseguridadtotal .
2. Identifíquese con el usuario y contraseña de telefonicaonline.



3. Seleccione la opción ***Firewall*** del menú y pulse: Acceda a la gestión de Firewall❑

En cualquier caso, tanto si es usuario de ***Firewall***, del ***Pack Antivirus + Firewall*** o del ***Pack Seguridad Total***, aparecerá una pantalla similar a la siguiente:



4. Seleccione el apartado *Mis Servicios*.

5. Si se le pide, introduzca su dirección electrónica de suscripción y su contraseña y haga clic en **Conectar.**
6. Se activa el Asistente de instalación. Si no lo hace automáticamente, haga clic en Inicio.

Nota: si está actualizando una versión anterior, desinstalará automáticamente dicha versión antes de instalar la actual.

7. Una vez concluida la instalación se debe reiniciar el ordenador.
8. Después de reiniciar el ordenador, ya tiene disponible la funcionalidad.

❑ Configuración Inicial

Haga clic en el botón secundario del icono de McAfee situado en la bandeja de sistema y, a continuación, seleccione **Configuración del cortafuegos.**
A continuación, las principales características que puede definir un usuario del equipo en ***Firewall***:

Estado: Activado o Desactivado. Seleccione Activado.

Tipo de Conexión:

- o **Red fiable** (el equipo no puede comunicarse con otros equipos de la red local. Determinados servicios, especificados por el administrador, pueden tener acceso a Internet). Seleccione este tipo de conexión si está conectado indirectamente en una red separada de Internet por un cortafuegos o enrutador de hardware (*Router*). Por ejemplo: en una red doméstica o en la de la oficina.
- o **Red No fiable** (el equipo no puede comunicarse con otros equipos de la red local o de Internet). Seleccione esta conexión si está conectado directamente a Internet en, por ejemplo: a través de una conexión de marcación, una línea ADSL o un cable módem; mediante un tipo de conexión en un cibercafé, hotel o aeropuerto.
- o **Personalizada** (el equipo sólo puede comunicarse con aquellas direcciones IP y servicios especificados por el administrador). Seleccione esta opción si sólo debe permitir las comunicaciones desde servicios del sistema a través de puertos específicos o desde un rango específico de direcciones IP, o bien si se trata de un servidor que proporciona servicios del sistema.

Seleccione su caso y pulse aceptar.

Las siguientes aplicaciones, hasta que las defina cualquier tipo de usuario, están permitidas:

- ✓ MYAGTSVC (Agente Rumor)
- ✓ UPDDLG (Actualizar motor)
- ✓ MCUPDATE (Actualizar agente Virus Scan win32)
- ✓ MSTASK (SO Windows)
- ✓ MSDTC (SO Windows)
- ✓ SERVICES (SO Windows)
- ✓ RPCSS (SO Windows)
- ✓ TCPSVS (SO Windows)

Cualquier otra aplicación que trate de establecer una conexión a la red será bloqueada.

inicio

4. Uso

Haga clic con el botón derecho del ratón sobre el icono McAfee, coloque el puntero sobre ***Firewall.***

❑ Configuración de una conexión personalizada.

Si modifica la configuración de seguridad, puede configurar un tipo de conexión personalizada. El proceso de personalización permite designar lo siguiente:

- Puertos a través de los que el equipo puede recibir las comunicaciones, necesario para configurar el equipo como un servidor que proporciona servicios del sistema. El equipo aceptará las comunicaciones a través de un puerto abierto del equipo.
- Direcciones IP a través de las que el equipo puede recibir las comunicaciones, lo que permite limitar las comunicaciones a determinadas direcciones IP.

En el cuadro de diálogo **Configuración personalizada del cortafuegos**, puede definir con exactitud las comunicaciones que el servicio de protección de cortafuegos permite:

i. Configuración de los servicios del sistema para una configuración personalizada.

Determinadas aplicaciones, entre las que se encuentran servidores web y programas de servidor que comparten archivos, deben aceptar conexiones no solicitadas de otros equipos a través de los puertos designados de servicios del sistema. Al configurar un modo de funcionamiento personalizado, puede llevar a cabo lo siguiente:

- Permitir que las aplicaciones actúen como servidores en una red local o en Internet.
- Añadir o editar un puerto de un servicio del sistema.
- Desactivar o eliminar un puerto de un servicio del sistema.

Seleccione un puerto de los servicios del sistema sólo sí está seguro de que debe abrirse. No es muy habitual que necesite abrir un puerto. McAfee recomienda desactivar los servicios del sistema sin uso para evitar intrusiones.

A continuación se presentan ejemplos de servicios del sistema que generalmente necesitan que los puertos se abran:

- Servidor de correo electrónico: no es necesario abrir el puerto del servidor de correo para recibir los mensajes de correo electrónico. Es necesario abrir un puerto sólo si el equipo protegido por el servicio de protección de cortafuegos actúa como un servidor de correo.
- Servidor web: no es necesario abrir un puerto del servidor web para ejecutar un navegador web. Es necesario abrir un puerto sólo si el equipo protegido por el servicio de protección de cortafuegos actúa como un navegador web.

Puertos del servicio del sistema estándar.

Los servicios del sistema se comunican con Internet a través de los *puertos*, que constituyen conexiones lógicas. Los servicios habituales del sistema de Windows se relacionan generalmente con *puertos de servicio* particulares, y el sistema operativo del equipo u otras aplicaciones del sistema pueden intentar abrirlos. Teniendo en cuenta que estos puertos pueden

suponer una fuente de intrusiones para el sistema, debe abrirlos en la configuración predeterminada antes de que equipos externos pueden acceder a ellos.

Estos puertos de servicio estándar utilizados habitualmente se enumeran de manera predeterminada en el cuadro de diálogo **Configuración personalizada**, donde puede abrirlos y cerrarlos:

- Puertos 20-21 del protocolo de transferencia de archivos (FTP, File Transfer Protocol);
- Puerto 143 del servidor de correo (IMAP);
- Puerto 110 del servidor de correo (POP);
- Puerto 25 del servidor de correo (SMTP);
- Puerto 445 de Microsoft Directory Server (MSFT DS);
- Puerto 1433 de Microsoft SQL Server (MSFT SQL);
- Puerto 3389 de Remote Assistance/Terminal Server (RDP);
- Puerto 135 de llamadas de procedimiento remoto (RPC, Remote Procedure Calls);
- Puerto 443 del servidor web seguro (HTTPS);
- Puerto 5000 de Plug and Play universal (UPNP);
- Puerto 80 del servidor web (HTTPS);
- Puertos 137-139 de Windows File Sharing (NETBIOS).

Los puertos que no aparecen en la lista del cuadro de diálogo **Configuración personalizada del cortafuegos** no están supervisados por el servicio de protección de cortafuegos. Se permitirán las comunicaciones a través de los puertos que no aparecen en la lista. Para bloquear un puerto, debe añadirlo a esta lista y asegurarse de que se ha cancelado su selección.

Apertura de un puerto de servicio.

1. Haga clic con el botón secundario en el icono de McAfee situado en la bandeja de sistema y, a continuación, seleccione **Configuración del cortafuegos**.
2. En la ficha **Configuración**, seleccione la zona **Configuración personalizada**.
3. Haga clic en **Editar**.
4. En el cuadro de diálogo **Configuración personalizada del cortafuegos**, seleccione las casillas de verificación situadas junto a los puertos de servicio que desea abrir. El equipo aceptará todas las comunicaciones que se produzcan a través de estos puertos.

Seleccione un puerto en la lista **Nombre del servicio del sistema** sólo si está seguro de que se debe abrir. McAfee recomienda desactivar los servicios del sistema sin uso para evitar las intrusiones.

5. Haga clic en **Aceptar**.
6. En la ficha **Configuración**, seleccione **Aceptar**.

Adición y Edición de puertos en servicio.

1. Haga clic con el botón secundario en el icono de McAfee situado en la bandeja de sistema y, a continuación, seleccione **Configuración del cortafuegos**.
2. En la ficha **Configuración**, seleccione la zona **Configuración personalizada**.
3. En el cuadro de diálogo **Configuración personalizada del cortafuegos**, haga clic en **Agregar** o seleccione un servicio existente y haga clic en **Editar**.
4. En el cuadro de diálogo **Conexión entrante**, especifique el nombre del servicio.
5. Especifique los puertos a través de los que este servicio se comunicará
6. Seleccione el protocolo (“idioma”) que el servicio utiliza para establecer la comunicación. Consulte la documentación de la aplicación si no está seguro de el protocolo que debe seleccionar.
    - **TCP**: el protocolo de control de transmisión/protocolo de Internet es el protocolo de Internet más común y se puede utilizar como protocolo de red.
    - **UDP**: el protocolo de datagramas de usuario es menos sólido que el TCP/IP. Se utiliza habitualmente para intercambiar pequeñas unidades de datos entre el equipo de una red que utiliza el protocolo de Internet.

- **Ambos**: TCP y UDP. Haga clic en **Aceptar**.

Nota: si la documentación de la aplicación no especifica el protocolo, McAfee recomienda la selección de TCP/IP, ya que se trata del protocolo más utilizado. No seleccione Ambos si no se precisan los dos protocolos, ya que, de esta manera, la red será más vulnerable a las intrusiones.

7. En el cuadro de diálogo **Configuración personalizada del cortafuegos**, seleccione las casillas de verificación situadas junto al servicio.
8. Haga clic en **Aceptar**.
9. En la ficha **Configuración**, seleccione **Aceptar**.

Para cerrar un puerto de servicio.

1. Haga clic con el botón secundario en el icono de McAfee situado en la bandeja de sistema y, a continuación, seleccione **Configuración del cortafuegos**.
2. En la ficha **Configuración**, seleccione la zona **Configuración personalizada**.
3. Haga clic en **Editar**.
4. En el cuadro de diálogo **Configuración personalizada del cortafuegos**, seleccione un servicio de la lista y, a continuación, haga clic en **Eliminar**.
5. En el cuadro de diálogo **Configuración personalizada del cortafuegos**, haga clic en **Aceptar**.
6. En la ficha **Configuración**, seleccione **Aceptar**

ii. Configuración de una dirección IP para una configuración personalizada.

Además de aceptar las comunicaciones a través de los puertos de servicio seleccionados, el equipo aceptará las comunicaciones que se originen desde las direcciones IP designadas.

1. Haga clic con el botón secundario en el icono de McAfee situado en la bandeja de sistema y, a continuación, seleccione **Configuración del cortafuegos**.
2. En la ficha **Configuración**, seleccione la zona **Configuración personalizada**.
3. En el cuadro de diálogo **Configuración personalizada del cortafuegos**, seleccione las direcciones IP que pueden comunicarse con el equipo.
   - **Cualquier equipo**: todos los equipos y direcciones IP.
   - **Mi red**: todos los equipos con direcciones IP en la red local.
   - **Rango de direcciones determinadas**: sólo los equipos cuyas direcciones IP se hayan especificado aquí.
4. Haga clic en **Aceptar**.
5. En la ficha **Configuración**, seleccione **Aceptar**.

❑ Gestión de Aplicaciones de Internet.

Firewall supervisa las comunicaciones con las aplicaciones de Internet, que se conectan con Internet y su equipo. Cuando la protección de cortafuegos detecta una aplicación de Internet que se ejecuta en el equipo, permite que la aplicación se conecte a Internet o bloquea la conexión, en función de la configuración.

El usuario administrador puede configurar el servicio de protección de cortafuegos para permitir o bloquear determinadas aplicaciones de Internet, además de para solicitarle una respuesta siempre que se detecte una aplicación de Internet

¿Como responde ante una detección?

Cuando la protección de cortafuegos detecta una aplicación de Internet:

1. Comprueba la lista de aplicaciones que se han detectado en el equipo.

2. Comprueba la lista de aplicaciones que se han aprobado
3. Comprueba la “lista blanca” que se mantiene en el sitio www.hackerwatch.org de McAfee.
4. Si la directiva lo permite, le solicita una respuesta; de lo contrario, bloquea la aplicación

¿Cómo puedo gestionar las aplicaciones de Internet detectadas?
El servicio de protección de cortafuegos mantiene una lista de las aplicaciones de Internet que se han detectado en el equipo y que ha aprobado. Si la directiva así lo permite, podrá ver estas aplicaciones y sus permisos asignados. También puede editar los permisos o eliminar las aplicaciones de la lista.

Para gestionar las aplicaciones de Internet

1. Haga clic con el botón secundario en el icono de McAfee situado en la bandeja de sistema y, a continuación, seleccione **Configuración del cortafuegos**.
2. Haga clic en la ficha **Aplicaciones de Internet** para ver una lista de las aplicaciones.
3. Seleccione una aplicación para ver los detalles.
4. Para modificar el listado de aplicaciones:
   - Seleccione **Acceso completo** para permitir que la aplicación se comunique con Internet. La aplicación aparecerá en los informes administrativos como una aplicación aprobada por el usuario (también conocida como exclusión).
   - Seleccione **Bloqueado** para evitar que la aplicación se comunique con Internet.
   - Seleccione **Eliminar** para borrar la aplicación de la lista. La próxima vez que la aplicación trate de acceder a Internet, se le considerará una detección nueva, lo que quiere decir que la directiva determina la respuesta: la protección de cortafuegos bloquea la aplicación, solicita una respuesta o sólo registra el intento.
5. Haga clic en **Aceptar** para guardar los cambios.

inicio